Data Systems

A framework for the current state of the Tacoma Police Department

Table of Contents

Executive Summary

The foresight and efforts put into the strategic goal "to use data, information, and technology" in 2006 made TPD a regional leader in data driven policing. By 2011, the department to a large degree had obtained the goals set forth in the original strategic plan. This 2016 current state analysis examines "where we are today" regarding data systems and the "use of data, information, and technology". Although, still a regional leader in data-driven policing – changing technology and increased demand are progressively outpacing the capacity of TPD resources.

At the onset of this analysis, the team's assumption was "data systems" was synonymous with "software". The team soon discovered Data Systems extended far beyond software and its usage. Achieving this understanding required research, discussion with subject matter experts, and surveys, along with trial and error. Ultimately the team agreed that in the context of the department's 2006 strategic priority, Data Systems entails everything that supports data driven decision-making to fulfill the department's mission. Given the wide scope and complexities of this definition, the approach to uncover the current state of Data Systems required a holistic systematic examination to identify its basic structure even prior to identifying specific issues in very specific areas. This approach allows for root issues to be identified and addressed rather than immediate recommendations for the temporary treatment of specific topical symptoms. With this approach in mind, a framework for analysis was created from research and the related 2006 strategic goals.

There are three components within the Data Systems assessment framework that build upon one another -- **Coherent IT Infrastructure**, **Data Quality**, and **Data Exploitation**. A **Coherent IT infrastructure** is the foundation that enables consistent accessibility and transmission of data and information across a variety of different yet united platforms connections, data sources, software, and hardware both internally and externally. However, a solid foundation alone is not enough to be data driven. Good, quality data available and flowing across that coherent network is needed for good decisions and tactics. **Data Quality** refers to up-to-date, consistent, and accurate data that can be used to support operational, tactical, and strategic department efforts. Network connections, speeds, and data quality feed into the exploitation of data which in turn either help or hamper our data driven efforts. **Data Exploitation** is using the data to answer questions, drive decisions, and support operational, tactical, and strategic department efforts at all levels to empower problem solving. Tools and systems deliver the actionable data to the user to accomplish this. This report is a high-level assessment using this framework and these three focus areas.

At a high-level or macro-level, TPD has the foundational pieces in place to be an optimized data driven organization, but technical and cultural weaknesses, along with capacity issues are impeding organizational growth. Regarding the need for a Coherent IT Infrastructure, the findings of our research reiterated the complexities and interdependencies between TPD's infrastructure and its external partners at the federal level (e.g. Federal Bureau of Investigations), state level (i.e. Washington State Patrol, Washington Association of Sheriffs and Police Chiefs), and local level (i.e. Pierce County, SouthSound911 and City of Tacoma). TPD cannot have a Coherent IT Infrastructure without these external partners. Needed support from City of Tacoma IT and SouthSound911 is limited because a mutual understanding of individual agency needs and priorities is lacking between the entities. Internal capacity is strained, while both internal and external demand increases. Existing and newly created federally unfunded mandates and initiatives (i.e. FBI's CJIS requirements, White House Data Initiative) put a greater strain on department resources. The increase in demand is further driven by external expectation for transparency, accountability, evidence-based practices, and efficiency in policing and government

(i.e. Project Peace, the City Manger's Performance Measures, and The President's Taskforce on 21st Century). This in turn, helps drive the internal expectation, as evidenced with TPD's Tacoma Crime Control System, which promotes collaboration, responsibility, and effective responses using data to address crime problems. Bad data or poor data quality hinders meeting these demands and expectations. Further, poor data quality is undermining the current set of tools available to department employees. Despite our data quality issues, available tools are underutilized due to a lack of understanding and training. This appears to be both a technical and cultural issue coupled with the lack of available proactive time for officers. TPD's overall maturity level as a data driven organization, seems to have stalled while trying to move towards standardizing and optimizing the "use of data, information, and technology".

Ultimately, the recommendations of where we head in the future are driven by the department's vision and desired level of data driven maturity. Given the foundational pieces in place from the 2006 strategic goal, there is great potential for growing into a world class data driven police agency. It is recommended TPD complete a more in-depth analysis on each of the components of the data driven framework -- **Coherent IT Infrastructure**, **Data Quality**, and **Data Exploitation**, drilling down into each area as determined by the department vision. Systems and process improvements can then be identified and implemented for efficiency in each area of the framework. In the interim at this macro-level there are steps that can be taken to support each of these three areas that would improve bottlenecks and alleviate some of the strain and symptomatic issues. This in turn, would free up more FTE time to handle additional symptoms. For example, seeking strategic alignment with our external partners is key to prioritizing support for our department's continuous operations of the IT infrastructure and addressing data quality issues to meet our department's needs. Additionally, the education and training of department members on available tools, how to use data and information, and connecting individual efforts with the department's goals is paramount to furthering the Tacoma Police Department maturity as a data driven organization. The attached report looks into each of these areas in greater depth and provides further recommendations to becoming a world-class data driven organization.

Introduction

Background

Information is critical in law enforcement. The ability of law enforcement to fulfill its public safety responsibility relies on increasing citizen and officer safety and using resources more effectively. Information and technology drive this ability. The timely access to accurate information by all parties is key to accomplishing this mission. In 2006, the Tacoma Police Department (TPD) created a Strategic Plan where the first priority was to "use data, information, and technology" [1] and outlined the foundational pieces to become a data driven organization. Being data driven allows decision-making at all levels of the department to be more effective. This current state analysis on data systems corresponds to this strategic priority. A framework for analysis and macro-level assessment of factors that are currently affecting or will affect the organization's ability to fulfill its mission are examined in this document. This is a critical step in the strategic planning process by providing feedback, helping shape priorities surrounding data driven decision-making, and ultimately fulfilling the organizational mission to achieve a desired future.

Definition

The scope and concept of data systems is broad and to a large degree, abstract and intangible. Developing a common understanding of data systems required research, discussion with subject matter experts and a cross section of capable employees that comprised the team, coupled with trial and error. In the context of the department's 2006 strategic priority, data systems entail everything that supports data driven decision-making to fulfill the department's mission. It can involve hardware used to input the data, store the data, or a device to deliver the data to an end user; it could be software that captures the input and provides an interface to access the data; or a process or workgroup that adds value to the data to create information. Further, the information produced must be utilized to inform decisions and guide police actions.

Complexity

The interconnectedness and multidimensional nature of data systems made the initial attempts at a micro-level examination, intended on producing data driven results, difficult. At the onset of this project, there was a software-oriented bias that came to light through attempts at developing a survey on the department's available software and tools. On the surface it seemed straightforward -- a system, tool, and/or software is either used or it is not. However, research from different industries indicated otherwise. There are multidimensional aspects of use - mandatory versus voluntary, informed versus uninformed, and effective versus ineffective [2]. Further, there is the *Intention to Use* which is about an attitude, whereas *Use* is behavioral. A quantitative approach through the use of a survey could not capture the detail and dimensions needed for the meaning and conclusions being sought in current state analysis. Additionally, for the survey to solicit accurate responses, questions and survey variables need to be explicitly defined and understood by respondents. Testing the survey instrument revealed a lack of both general understanding of the data systems concept and specific nuances between definitions which would ultimately lead to false conclusions based on the results.

Evolution

To unravel the complexities, a new approach needed to be adopted. Rather than focusing on specific symptoms of many systems to make general conclusions with an inductive approach -- the focus shifted to a deductive approach

beginning at the macro level, seeking to identify the basic structure and current state of the overall system in place, while allowing for the ability to drill down further at a later date. This approach delivered a more systematic way of looking at the system and the identification of its various components, practices, procedures, partners, and stakeholders. The new approach addresses root issues prior to smaller issues for long-term effectiveness.

Data driven decision-making requires more than good data for good decisions. An infrastructure and systems to capture, deliver, and leverage the data are paramount for success. Thus, a framework for data driven decision-making entails three components or aspects -- **Coherent IT Infrastructure, Data Quality,** and **Data Exploitation** [3]. Additional research outlined the different dimensions within these aspects to gain a thorough understanding of the current state of Tacoma Police Department data systems. The dimensions or criteria for each component are discussed in the following sections.

Assessment

Framework

Empirical research and qualitative methods -- group discussion, survey questions, etc. -- shaped the framework which consists of three components -- **Coherent IT Infrastructure, Data Quality,** and **Data Exploitation** adapted from *Data Driven: Profiting from your businesses most important asset*. Further research was conducted on each of these areas to generate deep dive areas of exploration. These three components in the original framework instantly resonated with the group, as it articulated the different priorities and positions that each of the group members brought to the table, as a holistic framework.

The use of this framework aligns with the 2006 strategic priority regarding the "use of data, information, and technology" and the five goals within this department priority [1]. Each of which is driven by one or more of the three components of our framework (see Table 1). For example, the overt component relating to the 2006 strategic priority for using data, information, and technology and adopting a data driven approach is **Data Exploitation**. It was recognized in 2006 that department units needed to be created or enhanced to achieve a data driven approach to crime management. Having a "progressive IT department" is dependent on an interconnected **Coherent IT Infrastructure** as a foundation to be successful. While the creation of the "Crime Analysis Unit" would support the goals of creating a "leadership dashboard" and "comprehensive data driven approach" through the data analysis. Both work units were the catalysts for the creation of "effective data systems" to be used for **Data Exploitation**. The **Data Quality** component is not explicitly stated in the 2006 goals, though it underpins each of the goals, and without it undermines efforts to succeed in these areas.
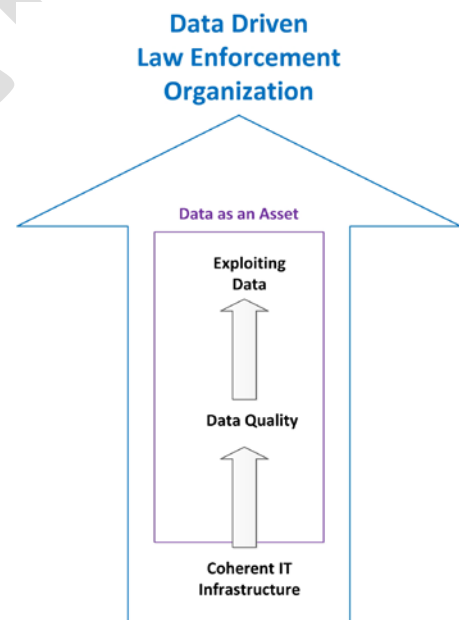

Figure 1. Data Systems Framework

Table 1.

Goal #	2006 Strategic Goal	2016 Framework	
		Primary Component	**Secondary Component**
1.	Create a Crime Analysis Unit	Data Exploitation	Data Quality Coherent IT Infrastructure
2.	Develop comprehensive data driven approach to crime management	Data Exploitation	Data Quality Coherent IT Infrastructure
3.	Create progressive IT department within TPD that capitalizes on technology	Coherent IT Infrastructure	Data Exploitation
4.	Create effective internal data systems	Data Exploitation Data Quality Coherent IT Infrastructure	
5.	Create/implement leadership dashboard	Data Exploitation	Data Quality Coherent IT Infrastructure

Coherent IT Infrastructure

A Coherent IT Infrastructure is logical, consistent, and united throughout a variety of different connections, data sources, software, and hardware. This infrastructure is the foundation that enables accessibility and transmission of information to make decisions regardless of the tool being used. TPD is unique in that it is heavily reliant on three different IT entities – TPD IT, City of Tacoma (COT) IT, and South Sound 911 (SS911) IT for providing its infrastructure, systems, and services. There are also integration needs with other external connections at the local, state, and federal levels to provide access and information sharing between agencies.

System quality and service quality have been shown to directly affect use and user satisfaction, which in turn affects the ability to leverage information at all levels of law enforcement [2]. This includes common IT issues such as interconnectedness between systems, dropped connections, system bugs, speed, and access. Dropped connections, network degradation, connection speed, and other IT issues hamper employee productivity in any department, but with policing it has public safety consequences. TPD has recently experienced this where network degradation occurred on the City IT infrastructure, limiting the ability of officers to connect to SS911 applications and complete essential functions of their job. This is not in alignment of the National Security Presidential Directive-51/Homeland Security Presidential Directive-20 (NSPD-51/HSPD-20) where organizations must incorporate redundancy and resiliency as a means and an end.

An adequate amount of capable staff is needed to support basic IT endeavors in a timely manner. TPD IT is responsible for maintaining desktop computers, cell phones, laptops, servers, and printers for TPD. The demands on TPD IT have exceeded the current unit capacity. There are 93 work tickets [4] backlogged for TPD IT. It is suggested that 4.8 IT staff members would be the average needed for an organization with 250-499 employees [5].

TPD IT has two employees -- one Computer Services Technician and one Senior IT Analyst (see City of Tacoma website for Job Specifications). There is no additional coverage if one or both of the IT employees are unavailable.

The potential effects of IT systems on policing are driven by the policing activities and management philosophies of individual agencies [6]. How information is used for reactive response to incidents is significantly different from how information is used for proactive and community-policing activities [6]. Advanced activities, analysis, and expectations -- like those associated with being a data driven organization, create a greater demand on IT than purely supporting operational functions (i.e., functioning printers, maintaining computers, etc.). With the strategic priority of using data, information, and technology and the adoption of the Tacoma Crime Control System (TCCS), the Tacoma Police Department has instituted both proactive and community oriented approaches. Producing and utilizing real-time information for assessment, along with both internal and external collaboration has an impact on the infrastructure and the support of systems that facilitate the activity and police response. TPD has a greater demand on support units than other law enforcement agencies who have yet to adopt proactive policing philosophies.

The previously mentioned connectedness and reliance on the different IT entities for parts of the TPD IT infrastructure creates additional complexity and barriers. The span of control on IT aspects varies by function and is influenced by relationships and politics. The different IT entities have different priorities. The different priorities affect the responsiveness in supporting the needs of TPD both strategically and in its daily operational needs. Top priorities for TPD may fall to a secondary priority of another IT department as they manage their own priorities. Additionally, with the three different IT entities there is confusion by users of knowing who to contact with issues. This is a source of frustration by users and TPD IT then becomes the point of contact to resolve the issue even if they are not the responsible party.

Additionally, the Federal Bureau of Investigation (FBI) has created unfunded federal security guidelines regarding Criminal Justice Information Services (CJIS) and any technology related to it. The essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of all criminal justice related information. The CJIS Security Policy provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of criminal justice information through 13 different policy areas. This policy applies to every individual -- contractor, private entity, noncriminal justice agency representative, or member of a criminal justice entity -- with access to, or who operate in support of, criminal justice services and information [7]. These requirements create external demands on the TPD IT unit. Partner entities that do not follow CJIS requirements cannot provide support to handle these additional demands.

There appears to be a lack of mutual understanding regarding the priority of CJIS requirements between COT IT and TPD IT. Only a few COT IT personnel have the requisite fingerprint and background checks required by CJIS policy 5.12.1.1 to provide support to TPD. TPD is not able to receive the same level of IT support from COT IT as other city departments who don't have CJIS requirements and the need for backgrounded personnel. The $4,000 per computer (laptop and desktop) flat rate assessed to the police department per biennium to cover bundled services such as PC Support, Network Connectivity, and Email Support [8] is a source of frustration, as the PC Support function has to be provided by TPD IT. PC Support from TPD IT is an additional cost to the department on top of the flat rate assessment. Current COT IT capacity dictates that even if staff were CJIS-compliant, Computer Support Technician onsite support to TPD would have to be provided off-shift, with TPD paying their on overtime. With two TPD IT personnel, this has created a backlog with TPD's 450 devices that have to be maintained and

upgraded internally. Addressing the unfunded CJIS mandates increases the demand on the limited TPD IT staff, while simultaneously limiting support that can be provided by COT IT. This creates further strain on TPD IT staff's ability to support department IT functions.

The Tacoma Police Department is currently in violation of the Federal Bureau of Investigation's CJIS mandates. The two-factor authentication project -- a collaboration between COT IT and TPD IT -- is overdue from the original deadline of April 2015 and the updated extended deadline of December 2015 [9]. Additionally, as a Criminal Justice Agency (CJA), CJIS requires TPD's network to become isolated from the City of Tacoma's (Noncriminal Justice Agency or NJCA) network in CJIS section 5.10. This will cause major infrastructure changes and costs. For instance, information posted on CopWeb content and most SS911 NetMenu applications are transmitting unsecured data between the SS911 and COT IT networks in violation of CJIS. The next FBI audit for CJIS is scheduled for February 2018. The FBI and its state liaison, the Washington State Patrol, have the ability to deny the Tacoma Police Department access to federal level data if TPD is not in compliance. This would include access to State Interface and National Crime Information Center (NCIC) -- officers would no longer have the ability to run vehicles or people to check on the vehicle's registered owner, the stolen vehicle status, violent criminal history or out-of-state warrant status of drivers. Not having access to this information would severely impact officer and citizen safety and limit investigative efforts -- both criminal investigations and background investigations for hiring police personnel.

Historically, the Law Enforcement Support Agency (LESA), now South Sound 911 (SS911), and the Tacoma Police Department were in strategic alignment regarding data systems under the Law Enforcement Activity and Data Systems (LEADS) plan 2007-2008. Its mission was to *provide and maintain accurate, timely, complete, secure, and cost-effective law enforcement business processes and information systems that support public and officer safety, operations, management, analysis, and planning* [10]. Changes in the level of support with current data systems and adopting new systems that do not meet TPD's needs have been an on-going issue. At the request of the SS911 Operations Board, SS911 created a Technology Program Management Committee in May 2016. Two Tacoma Police Department employees sit on this committee intended to guide the Operations Board. The sporadic meetings and low placement in the organization chart have generated an impression that the Technology Program Management Committee may not be fully utilized in bringing the entities into strategic alignment (see Appendix for organization chart).

Data Quality

To make data driven decisions, data is needed. To make well informed decisions, quality data is needed. Estimates have shown that 15-20% of the data in a typical organization is erroneous or otherwise unusable [11]. Poor data quality can immediately result in wrong or delayed decisions. Long-term consequences of poor data quality prohibit the organizations from trusting the data, finding new uses for the data, mining the data, and developing data driven strategies. Poor data quality affects the ability to automate queries and requires human intervention to fix errors prior to analysis, reporting, and accurate use, thus limiting the effectiveness of data driven analysis.

Data quality is an abstract, multi-faceted concept. While, data is an organizational asset, it is intangible and does not contain physical properties like those of other organizational assets (i.e., computers, cell phone, patrol cars, etc.). The threshold for acceptable data quality varies by use and information about data quality is hard to obtain. This is further complicated by the likelihood that most individuals entering data never see the effect of their errors downstream, and they don't fully understand the importance of good data. For instance, patrol officers may not

fully understand how their reports are being used by detectives, community liaison officers, and analysts to connect the dots or how the analysis of their reports are used by command staff to drive decisions, and answer city administration questions. TPD has created an awareness of the importance of quality data through departmental memos giving guidance, and training to new officers on available tools, in order to highlight the importance of complete and consistent data. These steps have helped improve specific issues with certain fields being filled in and proper coding selected, however, more work in this area is needed. There may be additional training opportunities for joining the importance of quality data into Enforcer with global departmental and city goals.

There are six core dimensions of data quality -- Completeness, Uniqueness, Timeliness, Validity, Accuracy, and Consistency [12]. These aspects also affect use and user satisfaction [2]. If data is redundant or obsolete, users won't trust or access the system. This is no different for police systems. A major complaint about the gang database was the information was not current. This impacted both the use of the system and the effort that was put into keeping the information current with the rationale of why input data and maintain it if no one is using the database. Additionally, workers spend 30% of their time searching for data they need [3]. Information is not always entered into optional data fields that are searchable by detectives or other officers. Other search tools like RSearch don't yield the expected results from the data and users are often left unsatisfied with the systems. In fact, poor data is the leading cause of many IT project failures[11] since poor data quality undermines the system and affects usage.

Additionally, there is a management aspect to ensure data quality. *Data Quality Management* entails the establishment and deployment of roles, responsibilities, policies, and procedures concerning the acquisition, maintenance, dissemination, and disposition of data [11]. A partnership between the user and technology groups is essential for any data quality management effort to succeed. Confusion regarding responsibility between these groups is cited as a common occurrence. The IT department assumes it's a user or department problem as long as they have the proper connection and devices, while the department or specific user group assumes IT is managing the data because "who else would be taking care of it?"[11, 14]. An illustration of this would be the assumption by IT that the quality of the data falls to officers filling out Enforcer reports, while the officers assume it is either TPD IT and SS911 ITs' responsibility to handle it. The new Computer Aided Dispatch system (CAD) deployed by SS911 has caused some data issues and necessitated the business group of the SS911 dispatch managers, SS911 IT staff, Tacoma PD analysts, and other analysts within Pierce County, to meet regularly to address these issues as no one group at the onset was responsible and each have different business and data needs.

There are two main approaches of ensuring data quality -- reactive or proactive [11] or simply put, finding and fixing errors or preventing them at the source. The proactive approach consists of establishing the overall governance, defining the roles and responsibilities, establishing the quality expectations, the supporting business practices, and deploying a technical environment that supports these business practices. This approach has not been adopted by SS911. Internally, the importance of correct data at entry has been recognized and intradepartmental memos emailed outlining expectations and/or encouraging fields in Enforcer reports be utilized in specific, known instances. This approach has been ad-hoc and needs-based, not a holistic adoption towards preventing data quality issues. This needs to be a partnership -- officers should understand the importance of good data and what it means to the organization, while IT can support this by implementing technology that facilitates quick and quality data entry and building in quality assurance steps or checks.

The reactive approach consists of dealing with problems that are inherent in the data in the existing databases. The majority of data quality management practices taking place are reactive and/or non-existent, both internally and externally for the available data to TPD. For instance, there is no quality testing or correcting by SS911 before they send the National Incident Based Reporting System (NIBRS) data to Washington Association of Sheriffs and Police Chiefs (WASPC) and eventually to the FBI. An initial check by TPD indicated that 1-2% of reported incidents credited to Tacoma did not occur within the jurisdiction due to the SS911 upload process not including quality control steps. Errors with the source data at SS911 leads the TPD CAU to perform their own reactive data quality approach. The Crime Analysis Unit as a whole spends time finding and fixing address errors. In addition, the unit is required to advocate for data quality with our internal and external partners, prepare data before it can be used for analysis, and deal with the absence of data which interferes with the ability to answer questions. These constraints affect the amount of analysis produced by the unit and also limits the ability for decision-makers to utilize "self-service" tools (e.g., Incident Mapping) for their own analysis. Poor data limits the effectiveness and use of available tools that support data driven decisions for officers at all levels of the Tacoma Police Department.

Data quality in systems that were developed without a data quality management program in place may be inadequate for meeting new needs [11]. Evolutions in technology and expectations create deeper needs from the data regarding data quality, in terms of specificity and the centralization of sources to be leveraged. Historical documentation for the LEADS project outlines the importance of data quality to LESA (SS911) as early as the strategic report for year 2000 [14]. The current state of SS911 strategic prioritization of data quality is not immediately known.

Data Exploitation

The exploitation or leveraging of data is the pinnacle to data driven decisions. Exploiting data at its most basic level is using data as information. This can be any form of analysis from simple searches to advanced statistics for strategic, tactical, investigative, administrative or operational purposes. Data exploitation includes the tools or software available to enable data driven decisions or support the business functions of the department, along with the education and training components to use information, and the level of organization-wide adoption of using data for decision-making. Leveraging data in policing is beneficial by:

- Solving crime -- connecting the dots
- Developing effective strategies and tactics to prevent future crimes
- Finding and apprehending offenders
- Improving safety and quality of life
- Educating the public
- Optimizing internal operations
- Prioritizing patrol and investigations
- Detecting and solving community problems
- Planning for future resource needs
- Enacting effective department policies

On its own, data does not drive decisions without analysis to create information, insight, or intelligence. TPD has software, tools, and employees dedicated to connecting dots, analyzing data, and delivering information to inform police action. As previously stated, data quality can undermine these tools and software and cause staff to spend more time looking for information or fixing data errors than analyzing data. If officers and analysts are spending

30%[3] of their time trying to locate data and/or can't find what they need, they can't exploit data. As a result, pertinent information may not get delivered, questions can't be answered, dots can't be connected, investigations might get stalled or delayed, or public and officer safety might be undermined. Automation of processes and "self-service" style analysis tools, like Incident Mapping and Hunch Lab, are hampered by poor data quality and in turn affect the volume of analysis produced. Poor data quality puts additional demands on the Crime Analysis Unit to fulfill the internal needs and requests that would otherwise be taken care of with the present tools available, ultimately limiting the volume of analysis produced to support other functions.

Using the metaphor of a clay sculptor, information can be built through adding different pieces together or chiseling away the extraneous [15]. There is almost never a piece of information just waiting for the question to be asked. WebRMS and calls for service data isn't stored or structured the way human brains or Google-type search engines work. Seemingly easy inquiries, like "how many gunshot wounds have there been in 2015", is not a quick or simple question to answer, based on if and how the information is captured. To get an accurate number, it requires writing numerous database language queries to generate a list of possible candidate reports that have to be read through to get an accurate count, costing hours of an FTE time for this one question. Increasing amounts of internal and external requests for information and analysis generate additional demand on the Crime Analysis Unit, on top of their support of other organizational efforts (e.g., TCCS, Quarterly Reports, etc.), thus, limiting the volume and timeliness of analysis produced. It is recommended to have one crime analyst for every 70 officers, depending on the level of advanced analysis and efforts desired by the police administrations [16]. For an agency the size of Tacoma that equates to 4.8 Crime Analysts, not adjusting for the desired level of advanced analysis. Currently, the Crime Analysis Unit has one Senior Crime Analyst (unit supervisor) and one Crime Analyst, along with two Crime Program Technicians who support the Crime Analysts (see City of Tacoma website for Job Specifications).

Tools and software provide the vehicle for data driven efforts. The use of these tools drives many of the efforts. On the surface, it seems straightforward that a system, tool, and/or software is either used or it is not used, but there are multidimensional aspects of use. Additional factors such as information quality, systems quality, and service quality affect use and user satisfaction. Tools and software may be used for a variety of business processes by multiple users at any given time regardless of the original purpose of the software. This co-opting of the tool to meet changing needs may result in a variety of complaints or problems for one user for one purpose, but may be a necessity for another user to complete a different function. This same thought can be used for volume of usage. One employee may need a system for 100% of their job while 100 employees may only need the system for 10% of their job function. Great consideration is needed when evaluating software, tools, and systems that support data driven decisions. Fortunately, models exist for measuring the complex-dependent variables that determine the success of an information system [2].

Education and training is paramount to data exploitation. There is a technical aspect that requires knowing what tools exist, how to use the tools, and the limitations of those tools. Education on how to interpret and use information is also key for being a data driven organization. To measure outcomes of efforts, planning and design needs to happen before the effort starts. Not understanding or capturing the right data can lead to either wrong conclusions or the results not being utilized at all in the decision-making process. False conclusions may lead to incorrect tactics being selected, which has a cost in wasted resources, and may undermine the perception of the effectiveness of either the tactic, the program, or the data driven process itself.
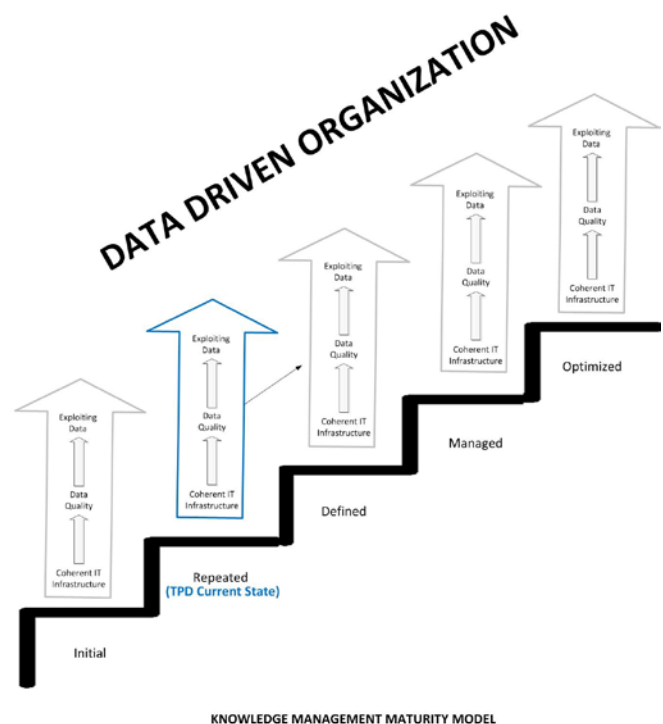
How data is presented greatly affects how it is understood. If it is not presented at the level the decision-maker needs it, whether that be a level too high to be actionable or too granular where the bottom line is lost, the data may be reviewed but disregarded. Ideally, a culture of inquiry [17] and using data should be at all levels of the department, across all work units. Unfortunately, there is not a one-size-fits-all approach to data exploitation. Different levels have different needs and different decisions to make. For instance, a lieutenant needs a more granular level of information about division activities than the bureau chief because each have different responsibilities and decisions to make. This is similar to the Stratified Model [16], where there is a variable scope from short-term individual or groups of incidents to long-term more complex problems, which both require a layered but integrated approach for organizational crime reduction strategies and accountability. Each level builds upon the previous one, becoming more global.

There is a cultural aspect to using data and knowing the relevance of using data. The decision-maker may interpret the messaging of data driven as taking precedence over their own knowledge and experience, rather than complementing it. This can affect the level of adoption or "buy-in". Data and its subsequent analysis, should be used to compliment the experience, not replace it. It can provide objective frameworks that reduces the risk and uncertainty in decision-making [3] leading to better understanding, increased prioritization, and optimizing of resources for effectiveness. Connecting the individual effort to the bigger picture and educating staff on the strategic goals and their role in achieving these goals will alleviate friction and cultivate growth as a data driven organization. For instance, in the case of TCCS, the common theme was that many employees had heard of it but didn't know what it really was or how it pertained to them. Education would close this gap.

Data Driven Maturity

The Data Systems framework can be applied to part of a larger concept that models the level of adoption by an organization being data driven. The level or maturity of a data driven organization illustrates the steps or prevalence towards organization-wide use. Team research found that there are several different maturity models, all with some overlapping components but different emphasis points. There were no applied models or examples for law enforcement agencies found in the team's research. Research regarding the increase in analytical capacity is limited to CompStat or ad-hoc practices geared towards individual evidence-based policing strategies. Most maturity model examples were found in the private sector but offer general application to law enforcement.

The *Siemens AG (2000) Knowledge Management Maturity Model* [18], was one of the first and probably most general models available. There are five maturity levels of Organizational Knowledge Management. The first level is *Initial*, where the activities are non-systematic and ad-hoc. The second level is *Repeated*, which includes pilot projects and regular, individual activities. *Defined* is the third level, with standardized processes created, governed, and optimized regarding the use of data driven decision-making and knowledge

KNOWLEDGE MANAGEMENT MATURITY MODEL

management. The fourth level is *Managed* where the creation, sharing, and use of knowledge and data driven efforts is organizationally integrated and improved through measurement. The last level of maturity is *Optimized*. This level builds upon *Managed* with continuous development of efforts, as the organization strives for world-class status.

Topically applying the above model to TPD, the department seems to have successfully *Repeated* data driven efforts on the second level. It has moved towards the third step of *Defined*, with standardization of processes being created through TCCS, but additional work needs to be done towards governance of how data driven efforts are measured and optimized to complete the third level and move on to the fourth level with organizational integration. Completing a thorough assessment of the maturity of the Tacoma Police Department through the documentation of training, projects, measurement, integration of all the data driven efforts, and decision-making would be beneficial to create an organizational benchmark.

Recommendations

How data driven does the Tacoma Police Department want to be? That's the big question that needs to be answered. With the foundational pieces built from the 2006 Strategic Plan, TPD is in a strong position to be a nationwide leader in data driven policing. However, external requirements, such as CJIS, the White House Data Initiative, and higher expectations from the federal level (e.g. The President's Taskforce on 21st Century Policing), the state level (e.g. Washington State Executive Order 13-04), and the city (i.e. Project Peace and Performance Measures), create a growing demand on the department and its support functions for effectiveness, evidence-based practices, and government transparency. Meanwhile, ever-changing technology creates a moving target to maintain. This creates a situation where merely maintaining the foundational pieces will cause the department to be outpaced and systems to become stagnant. Therefore, being a data driven organization is an on-going commitment.

To create benchmarks and a road map to the future, **the overarching recommendation is to complete a deeper dive analysis on each of the three components -- Coherent IT Infrastructure, Data Quality,** and **Data Exploitation**. These areas need to grow together, as they are interconnected. The focus should be on treating the root causes and not just treating the symptoms to be truly effective. The depth and breadth of the analysis will need to be guided by the administration's desired level of being a data driven organization. To be an optimized, world-class data driven organization, it will require organization-wide efforts to achieve this goal and to change the culture. Idealistically, the most thorough level of analysis would be selected with the desire to be a fully optimized, world-class data driven organization. Realistically, the selection needs to be balanced and/or prioritized with the current workloads of the assessment team and external IT partners, and to an extent, the workloads of those expected to use the data, and other budgetary factors. The potential is great, but resources are not unlimited.

Conversely, a truly effective solution given the interconnectedness between IT infrastructures, responsibilities and intricacies of data quality, and multitude of components involved in exploitation, will not be easy. There is no one-thing quick-fix with systemic and cultural issues. However, there are immediate actions and recommendations in the short-term to alleviate some of the constraints on data systems that would also have a long-term impact.

The TPD IT unit needs additional resources to support the police department. Basic IT needs are not being met, let alone long-term strategic needs. That support may come from additional TPD IT staff or getting CJIS compliant COT

IT staff dedicated to providing the same level of support for the same cost as other city departments. Given the deadlines and requirements of CJIS, it is recommended to be a combination of both options, with a minimum of receiving one additional CST in TPD IT to free up the IT Analyst Sr. to focus on CJIS related matters to be in compliance by February 2018. The relationships between TPD IT and COT IT will need to improve and mutual understanding of priorities and needs should be outlined to make long-term strides. It is recommended that the COT IT department and Police Department strategically align their priorities in the near-term, since meeting CJIS deadlines for two-factor authentication and network isolation compliance is critical to the department.

Work has already begun with strategically aligning priorities with SS911 regarding data. Efforts have been made by all parties regarding specific data quality issues and working towards solutions, data definitions, and towards mutual understanding. It is recommended to formalize the strategic alignment with SS911 and work together in the deep dive analysis of data quality. This would help identify officer training issues with entering data into Enforcer, create baselines for data quality, and explore the adoption of proactive data quality approaches to prevent errors (e.g. make it easier for officers to enter in data with tools or apps that can scan a driver's license to autofill information into Enforcer reports). Though extremely beneficial, this would require resources from both parties to accomplish -- whether that be in changing the priorities for current staff or adding dedicated personnel such as a data steward. Increasing data quality will increase the amount of analysis produced by freeing up CAU staff time currently spent fixing data, provide quicker turnaround in finding data, and empower the current available tools.

The cultural and technical education and training of available tools, how to use data and information, and connecting individual efforts is paramount. Initial steps to train employees on what TPD currently has available and department efforts, such as TCCS, would have long-term benefits. Developing a basic training on using data and information in decision-making would optimize what the department is currently doing, and build capabilities in the long-term, regardless of the future data driven outcome chosen. Further exploration in exploiting data is a necessity to avoid counterproductive action and undermine the overall vision. For instance, it may be counterproductive to train all employees to use information and analysis, when doing so simultaneously limits the amount of analysis produced given the limited staff in this subject area. Generating benchmarks and interim goals supported by command staff will mitigate these types of issues.

The Tacoma Police Department has been a regional leader as a data driven organization because of the strategic goal created in 2006 of using data, information, and technology. TPD has the potential to be one of the best in the nation, but resources are needed to create the next strategic vision for the future.
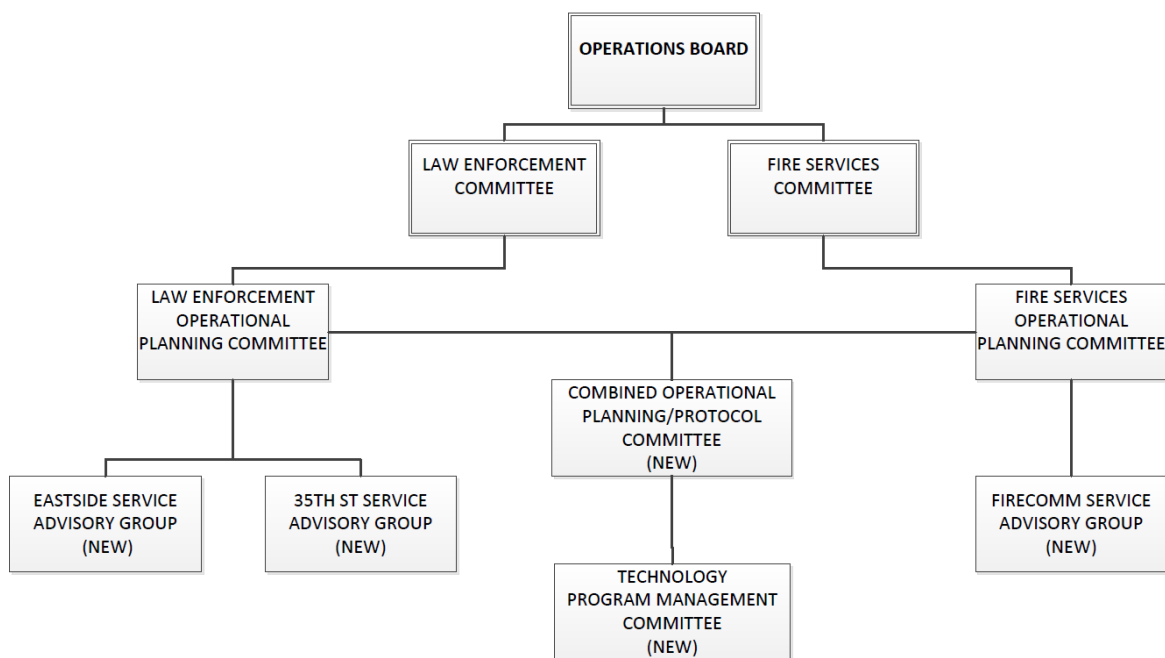
Appendix

References

[1]   Tacoma Police Department (TPD) Strategic Plan (2006).

[2]   DeLone, W. H., & McLean, E. R. (2003). The DeLone and McLean Model of Information Systems Success: A Ten-Year Update. Journal of Management Information Systems, 19(4), 9-30.

[3]   Redman, T. C. (2008). Data driven: Profiting from your most important business asset. Boston, MA: Harvard Business Press.

[4]   As of August 15, 2016 per email from TPD IT Analyst Sr.

[5]   McLellan, C. (2014, October 1). IT budgeting in 2015: What the surveys tell us. Retrieved June, 2016, from http://www.zdnet.com/article/it-budgeting-in-2015-what-the-surveys-tell-us/

[6]   Jackson, B. A., Greenfield, V. A., Morral, A. R., & Hollywood, J. S. (2014). Police Department Investments in Information Technology Systems: Challenges Assessing Their Payoff. Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR500/RR569/RAND_RR569.pdf

[7]   United States Department of Justice – Federal Bureau of Investigations (2016). Criminal Justice Information Services Security Policy, Version 5.5. Retrieved August 10, 2016, from https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

[8]   City of Tacoma IT Department cost booklet – Draft Version, 2016.

[9]   TPD IT per email from TPD IT Analyst Sr.

[10]   LEADS Strategic Plan 2005-2006.

[11]   Geiger, J. G. (2004). Data Quality Management: The most critical initiative you can implement. SUGI29, Paper 098-29. Retrieved April, 2016, from http://www2.sas.com/proceedings/sugi29/098-29.pdf

[12]   International Data Management Association (2013). The six primary dimensions for data quality assessment: Defining data quality dimensions. Retrieved April 01, 2016, from https://www.dqglobal.com/wp-content/uploads/2013/11/DAMA-UK-DQ-Dimensions-White-Paper-R37.pdf

[13]   National Association of State Chief Information Officers (2015). Managing Data as a Strategic Asset: How is that accomplished? Retrieved from http://www.nascio.org/dnn/portals/17/2015MY/Managing%20Data%20As%20a%20Strategic%20Asset.pdf.

[14]   LEADS Strategic Plan 2000.

[15]   Bruce, C. W., Hick, S.R., & Cooper, J. P. (2004). Exploring Crime Analysis: Readings on Essential Skills. North Charleston, SC.

[16]   Boba, R., & Santos, R., 2015. A Police Organizational Model for Crime Reduction: Institutionalizing Problem Solving, Analysis, and Accountability. Washington, DC: Office of Community Oriented Policing Services.

[17]   Changing Culture. (n.d.). What Works Cities.

[18]   Ehms, K. (2001). Holistic development of knowledge management with KMMM. Retrieved from http://www.kmmm.org/objects/KMMM_WC_on_IC2001_2001-01-18.pdf.

Strategic Goal Team Members

Assistant Chief Pete Cribbin .... Sponsor
Lieutenant Bob Maule .... Lead
Crime Analyst Sr. Jacquie Shelton .... Crime Analysis Unit
Crime Analyst Megan Yerxa .... Crime Analysis Unit
Detective Jared Matheson .... Criminal Investigations
PASS Angie Skrabak .... Criminal Investigations
Forensics Supervisor Paul DePoister .... Forensics
IT Analyst Sr. Guy Bollinger .... Information Technology Unit
Lieutenant Chris Travis .... Patrol/Special Investigations

SS911 Operations Board Committee Org Chart

2006 Strategic Goal Status

Strategic Priority	Goal	Expected Outcome, Measures, Milestone	2016 Status
Utilize data, information, and technology	Create crime analysis unit	• Unit fully functioning • Databases established • Report data accurate and consistent • Real time data accessible to all • Data analysis available	• Depends on the definition of fully functioning but the unit is maximized in its capacity • Databases been established and created • Unit has made accuracy and consistency a priority through standardization and SOPs • 20-25% of time spent cleaning data • Real time data only accessible through limited tools • Analysis is available
	Develop a comprehensive data-based approach to crime management	• Overall crime control strategy established • All TPD personnel understand the philosophy, goals, and their own roles and responsibilities in support of the philosophy • Organization structured to support the comprehensive approach. • Data strategically utilized to reduce and prevent crime and for directed enforcement • Resources deployed based on data • Sector based crime control strategies and dashboards in place • Effectiveness measures identified	• Currently reestablishing • People trying to understand roles and responsibilities but limited to command level only • Different units may not know much about TCCS • Limited capacity to support comprehensive approach • Is used ad-hoc • Tools are present but unsure about the level of adoption • Data not captured for measurement
	Create a progressive IT department that capitalizes on technology	• Fully functioning, capable IT department in place • Department's mission, roles, critical competencies, resources identified • TPD aligned and integrated with City IT • Technical support provided for crime control strategy • Positive representation with LESA programs • TPD utilizing state of the art technologies to reduce crime and operate efficiently	• Capacity strained, not fully functional • TPD not aligned and integrated with City IT • Have some state of the art technologies but the level of adoption is uncertain
	Create effective internal data systems	• Internal data available to all critical users for decision making • Data supporting the efficient operations of TPD	• Doesn't appear to be available • Greatly strained by data quality
	Create/implement leadership dashboard	• Dashboard completed • Dashboard monitored monthly to track TPD effectiveness • Improvement strategies identified and implemented	• Dashboard completed • Current changes in data has caused challenges in obtaining the data from all data sources • Uncertain if strategies have been identified and implemented